Volume 9, Issue 44 Atari Online News, Etc. November 2, 2007

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #0944 11/02/07

~ Famicon: End Of Road? ~ Simpsons Spoof Industry ~ OLPC Hits $200!

-* ICANN Group For Non-English! *-
-* More Spyware-Fighting Tools Needed! *-
-* Internet Ad Self-Regulation Falling Short! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""

Well, with the coming of Daylight Savings Time this weekend, the fall season has really kicked in. Add to that some early-morning low temperatures (er, frost on the proverbial pumpkin!), more and more leaves falling to the ground, and the fact that we're in November!

This all also means that the golf season in New England is also winding down. In fact, most of us at my local course have been laid off for the winter. Heck, I've been laid off three times already in the past week! I'm hoping to be able to get in a few more rounds of golf before it really gets too cold (or dark) to play any more this season. In the interim, I guess I'll have some time to clean up all of these leaves, and devote some time to some more thought-provoking editorials! So, while I paw over some of the remaining Halloween treats left over (I always over-buy!), I'll leave you all to the rest of this week's issue. Oh, and don't forget to set your clocks one hour BACK this weekend and regain that extra hour of sleep Sunday morning!

Until next time...

=~=~=~=

PEOPLE ARE TALKING

compiled by Joe Mirando
joe@atarinews.org

[Editor's Note: Due to the relatively dearth number of messages in the Atari Newsgroups this past week, there will be no People Are Talking column this week.]

=~=~=~=

->In This Week's Gaming Section - "Simpsons" Video Game Spoofs Industry!
"""""""""""""""""""""""""""""" Famicom Faces End Of Road!

’Manhunt 2’ Rated ’M’!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
  """"""""""""""""""""""""""""""""""

"Simpsons" Video Game Spoofs Industry

In the latest antics of "The Simpsons," Bart chases a giant ape through a video game factory, Lisa destroys a logging camp and Marge storms city hall with an angry mob.

But don’t look for those episodes on TV.

They are levels in "The Simpsons Game" that hit stores on Tuesday amid praise from critics for its faithful recreation of the hit TV show’s look, feel and humor.

"That was one of the big design challenges on this game, to make each of the levels feel like episodes. We wanted to make the game feel like a fully playable season of the show," said Hans Tencate, lead producer on the game at Electronic Arts Inc.

Several writers from the TV show injected the game with the irreverent wit "The Simpsons" is known for, coming up with some 8,000 lines of dialogue - enough for a full season.

"Few games embrace their license’s soul so well - ’The Simpsons Game’ nails the show’s trademark humor, in-jokes, and social satire, plus it features impressive cartoony graphics and the real-deal voice actors. This is total fan service, meaning Simpsons fans - and apologists - will be pleased," gaming news site 1up.com said in its review.

The new game is the latest addition to the already large catalogue of more than 20 "Simpsons" titles, which range from 1991’s arcade machine to 2003’s "The Simpsons: Hit & Run."

But this appears to adhere most faithfully to the show.

Developers came up with a way that let them create Homer, Bart and other characters in 3D yet retain a look that is remarkably like the cartoony visual style of the show.

"It’s actually much harder to do than you would think partly because ’The Simpsons’ is hand-drawn. We came up with proprietary technology ... that gives the game a little more of what the TV show would look like," Tencate said.

The game hopes to build on two other milestones this year: the 400th episode of the TV show and the long-awaited movie adaptation that has pulled in more than $500 million at the box office worldwide.

In the game, the Simpsons discover they are living inside a video game and have powers matching their personalities. Bart, for example, can turn into the superhero "Bartman" while Lisa can activate the "Hand of Buddha" to move large objects.

Just as the show used a pop culture medium to skewer pop culture, the game is peppered with parodies of an industry still struggling to shed geeky stereotypes and win mainstream acceptance.

"There are not many video games to my recollection that do full-blown multilayered parodies of the video game industry. We make fun of everything from ’Pong’ to ’Tomb Raider’," Tencate said.

While the humor has won praise from critics, some reviewers said they were disappointed with some of the actual gameplay, the lack of online features and for limiting cooperative play to two people.

The game had an average rating of 69 on Metacritic.com, which creates a weighted average of reviews from gaming Web sites and publications.

ESRB Sticks By ’M’ Rating On ’Manhunt 2’

The board that assigns age ratings to video games will keep the "Mature" label on "Manhunt 2," resisting calls to raise it after hackers defeated measures that blur some of the game’s violence.

Patricia Vance, president of the Entertainment Software Rating Board, said Friday the rating "is still valid, and we stand behind it."

"Manhunt 2" went on sale in the U.S. on Wednesday for the PlayStation 2, PlayStation Portable and Wii game systems. On Thursday, publisher Take-Two Interactive Software Inc. confirmed that hackers had managed to unblur some gruesome scenes on the PSP version.

The hack only works on PSPs that have been modified to allow unauthorized content.

In the game, the player guides two people who escape from an insane asylum and go on a killing spree with a variety of implements, including axes.

When originally submitted to the ESRB earlier this year, the game received an "Adults Only" rating. Many stores refuse to carry games with that rating, so Take-Two made modifications, including blurring some details. The modified game was rated "Mature," which means it is intended for players 17 or older.

It is not the first time Take-Two and the designing studio, Rockstar Games, have been in trouble over game content. Two years ago, their game "Grand Theft Auto: San Andreas" shipped with a hidden sex scene that was easily unlocked by gamers.

In that case, the ESRB changed the rating from "Mature" to "Adults Only," causing retailers to pull it off shelves. It is now facing calls to do the same thing with "Manhunt 2."

"Not only should the AO rating immediately be reinstated on this game, the Federal Trade Commission should investigate Rockstar and the ESRB to determine how this was allowed to happen again," said California state Sen. Leland Yee, in a statement.

The demand was echoed by Common Sense Media, a San Francisco nonprofit that advises parents about entertainment that may be inappropriate for children. The ratings process lacks basic transparency, said Common Sense Media CEO James Steyer.

"We believe that families and all consumers should have an assurance from game publishers and the game ratings board that the content being advertised is the same as the content being sold," Steyer said.

The ESRB’s Vance said the PSP hack does not reverse all the modifications made to the game to take it from an "Adults Only" to a "Mature" rating.

She also said the "Manhunt 2" case differs from "San Andreas" because it’s much harder to restore the new game’s hidden content, and the publisher submitted all the content, even the parts that were obscured, for the ratings review.

"This is not a simple matter of unlocking content that’s easily accessible to anyone who has a PC or a PS2," Vance said. "Software and hardware is susceptible to illegal or unauthorized modification. As an industry, there are many measures that are taken to prevent that from happening, but there is no way to prevent it altogether."

She stressed that parents need to be vigilant just not about the games that children buy, but also what they’re downloading from the Internet or how they’re modifying their game hardware.

The board is a private, nonprofit organization founded by a game industry trade group.

Meanwhile, the National Alliance on Mental Illness condemned the game, saying it perpetuates the stereotype that the mentally ill are violent. It asked the publisher to further modify the game. Take-Two had no immediate response to that request.

Nintendo’s Classic Famicom Faces End Of Road

It could soon be game over for the Famicom, the vintage family computer that two decades ago set Japan’s Nintendo on a path to become a global video game icon.

Nintendo has decided to stop repairing the Famicom, the console that wowed the world with "Super Mario Brothers" and "Dragon Quest", because stocks of spare parts are running out, company spokesman Ken Toyoda said.

The family computer, which was sold as the Nintendo Entertainment System in the United States and Europe, made its world debut in Japan in 1983.

Boasting far superior graphics to any other home video game console on the market at that time, it went on to sell almost 62 million units worldwide, and was followed by the Super Famicom, repairs of which will also be halted.

"Some say it’s sad Famicom is leaving and players are nostalgic, but Nintendo’s saga has not ended. We want people to enjoy the Wii now," said the spokesman for the Kyoto-based firm, which began in 1889 making playing cards.

Nintendo can hardly keep up with demand for the Wii, which is known for its innovative motion-sensitive controller and aimed at customers who normally would not play video games.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Price Of MIT Professor’s "$100 Laptop" Hits $200

A computer developed for poor children around the world, dubbed ’the $100 laptop,’ has reached a milestone: Its price tag is now $200.

The One Laptop per Child Foundation, founded by MIT Professor Nicholas Negroponte, has started offering the lime-green-and-white machines in lots of 10,000 for $200 apiece on its Web site (http://laptopfoundation.org/participate/givemany.shtml).

Two weeks ago, a foundation executive confirmed recent estimates that the computer would cost $188, which was already higher than the $150 price tag in February and $176 in April.

The laptops are scheduled to go into production next month at a factory in China, far behind their original schedule and in quantities that are a fraction of Negroponte’s earlier projections.

It is unclear when the machines will be ready for customers, as the Web site said version 1.0 of the software that runs the machine will not be ready until December 7.

Foundation spokesman George Snell declined comment on the pricing or release schedule.

When Negroponte said he could produce the laptops for $100, industry analysts said it had the potential to shake up the PC industry, ushering in an era of low-cost computing.

He hoped to keep the price down by achieving unprecedented economies of scale for a start-up manufacturer, and in April, he told Reuters he expected to have orders for 2.5 million laptops by May, with production targeted to begin in September.

But that has not panned out. So far the foundation has disclosed orders to three countries - Uruguay, Peru and Mongolia. It has not said how many machines they have ordered.

Wayan Vota, an expert on using technology to promote economic development who publishes olpcnews.com, a blog that monitors the group’s activities, estimates orders at no more than 200,000 laptops.

"One-hundred dollars was never a realistic price. By starting with an unrealistic price, he reduced his credibility selling the laptop," Vota said.

Negroponte, a charismatic technologist who counts News Corp chief Rupert Murdoch and Mexican billionaire Carlos Slim among his friends, has attracted a lot of attention for the foundation.

He has met with leaders around the globe and promoted the introduction of computers into classrooms in the most impoverished regions of the world. As he has done that, big technology companies have boosted spending on similar efforts.

The laptop features a keyboard that switches languages, a video camera, wireless connectivity and Linux software.

Microsoft Corp is trying to tailor Windows XP to work on the machine and recently said it is a few months away from knowing for sure whether it can accomplish that task.

The display switches from color to black-and-white for viewing in direct sunlight - a breakthrough that the foundation is patenting and may license next year for commercial use.

The laptop needs just 2 watts of power compared with a typical laptop’s 30 to 40 watts and does away with hard drives. It uses flash memory and four USB ports to add memory and other devices.

Earlier this year the foundation teamed up with Intel Corp, which is developing a rival machine. The two may work together on a second-generation laptop. This first machine runs on a microprocessor developed by Intel rival Advanced Micro Devices Inc.

Whois May Be Scrapped To Break Deadlock

Tech industry lawyer Mark Bohannon frequently taps a group of searchable databases called Whois to figure out who may be behind a Web site that distributes pirated software or tricks visitors into revealing passwords.

Like a "411" for the Internet, Whois contains information such as names and phone numbers on the owners of millions of ".com" and other Internet addresses. Bohannon and his staff at the Software and Information Industry Association rely on the free databases daily in their efforts to combat theft and fraud.

Law-enforcement officials, trademark lawyers and journalists, as well as spammers, also use it regularly.

"The Whois database is in fact the best, most well-recognized tool that we have to be able to track down who in fact you are doing business with," said Bohannon, the trade group’s general counsel, adding that alternatives such as issuing subpoenas to service providers take more time and cost money.

Nonetheless, some privacy advocates are proposing scrapping the system entirely because they can’t agree with the people who use the system on how to give domain name owners more options when they register - such as designating third-party agents. Privacy advocates say individuals shouldn’t have to reveal personal information simply to have a Web site.

The so-called "sunset" proposal is expected to come up Wednesday before a committee of the Internet Corporation for Assigned Names and Numbers, or ICANN, a key Internet oversight agency.

It will have a tough time winning approval - and could create chaos. But the fact that abandoning Whois is on the table underscores frustrations among privacy advocates that ICANN appears on the verge of launching new studies and deferring a decision yet again after some six years of debate.

Ross Rader, a member of ICANN’s generic names council and the sunset proposal’s chief sponsor, said many negotiators are stalling because they prefer the status quo, which gives them the access to Whois that they desire.

An executive with domain registration company Tucows Inc., Rader said he is just trying to break the deadlock and doesn’t necessarily want the databases to disappear.

"What removing the status quo will do is force all of the actors to come together without the benefit of a status quo to fall back on and say, ‘We are now all screwed. What will we do?’" Rader said. "It will lead to better good-faith negotiations."

Think of it as saving the system by breaking it first.

Marilyn Cade, a former AT&T executive who has been active on Whois advocacy, called the sunset proposal "an emotional overreaction that somehow got crystalized into an option. Everyone who has done the long hours of hard work to examine policy options thinks that they have a monopoly on what is best, but the facts are not yet there."

Cade is part of the camp that prefers further studies on the extent of any Whois abuse and the degree to which individuals are actually registering names for personal use - which could justify more privacy - rather than for businesses, nonprofit endeavors or domain name speculation.

Those findings, she said, would help ICANN tailor new policies that address actual problems, even if it means delay. And the study option seems likelier than the sunset proposal to prevail Wednesday.

When the current addressing system started in the 1980s, government and university researchers who dominated the Internet knew one another and didn’t mind sharing personal details to resolve technical problems.

Since then, the use of Whois has changed greatly.

Law-enforcement officials and Internet service providers use it to fight fraud and hacking. Lawyers depend on it to chase trademark and copyright violators. Journalists rely on it to reach Web site owners. And spammers mine it to send junk mailings for Web site hosting and other services.

Internet users, meanwhile, have come to expect more privacy and even anonymity. The requirements for domain name owners to provide such details also contradict some European privacy laws that are stricter than those in the United States.

There’s agreement that more could be done to improve the accuracy of Whois, as scammers and even legitimate individuals who want to remain anonymous can easily enter fake data.

The disagreements are over "who gets to see it (and) how can we protect people’s privacy while at the same time making accurate information available to those who need it," said Vint Cerf, ICANN’s chairman.

ICANN’s Generic Names Supporting Organization Council appeared to break a logjam in March when it formed a working group to consider letting domain name owners designate third-party agents in Whois listings. Currently, owners must provide their full names, organizations, postal and e-mail addresses and phone numbers.

But when the working group started developing an implementation plan, the opposing sides quickly disagreed on the basics, including the level of detail required.

"There were a number of parties that just would not compromise and could not accept that there are legitimate uses of Whois," said Margie Milam, a working group member and general counsel of the brand-protection firm MarkMonitor.

Approval of the sunset proposal, as drafted, would mean abolishing the current Whois requirements by late 2008. After that, individual registration companies would be able to decide whether to continue offering data on their customers, leading to gaps in the registration records.

The threat of losing Whois would force serious negotiations before it happens, said Milton Mueller, a Syracuse University professor on the Whois working group. "The sense of shock that would settle around certain people would be rapid and immediate."

Whois Studies Approved, Privacy Deferred

A panel on Internet names voted Wednesday to defer long-simmering questions on whether names, phone numbers and other private information on domain name owners should remain public in open, searchable databases called Whois.

Instead, the committee of the Internet Corporation for Assigned Names and Numbers, or ICANN, decided on further studies, which privacy advocates consider a stall tactic after seven years of discussions so far.

The committee also rejected a proposal to give Internet users the ability to list third-party contacts rather than their own private data in the Whois databases.

Law-enforcement officials, trademark lawyers and journalists, as well as spammers, now access Whois to figure out who may be behind a Web site. But privacy advocates say individuals shouldn’t have to reveal personal information simply to have a Web site.

A third proposal, a so-called "sunset" option that would have allowed domain name registration companies to stop making the data available through Whois, was narrowly rejected, 13-10. That measure would have likely resulted in large gaps in registration records and was seen as a way to force concessions from current Whois users before the sunset actually takes effect.

Debate ran for about two hours, with the panel becoming bogged down at times on whether to amend the language of motions that had been slated for vote.

The proposal on listing third-party contacts was defeated 17-7, the same margin by which the studies measure was approved. The votes also had the effect of formally removing the Whois issue from the committee’s agenda, leaving it to ICANN’s board to decide whether and how to proceed further.

"We seem to be closing off the development process at the same time we’re opening the box to the same old debates that have been going on for seven years," complained Milton Mueller, a Syracuse University professor on the committee. "The whole world is watching now. ... They’re expecting ICANN to do something about this."

Ross Rader, a committee member who is the sunset proposal’s chief sponsor, said afterward that he was disappointed the committee opted for an "open-ended" study.

"We’ve had seven years of study on this issue ... What has not been answered is what are the specific questions we want answers to," Rader said. "From my perspective, further, broad, open study is just a way for (opponents) to say you don’t have enough votes to change the status quo."

The committee, the Generic Names Supporting Organization Council, set a deadline of Feb. 15 to identify what types of studies are needed.

Mike Rodenbaugh, one of the panelists representing commercial and business Internet users, defended criticism that ordering additional studies was "silly."

"We still see, obviously, very significant issues with Whois in general, and while there is sure to be debate on what precisely the scope of the studies (will be) ... almost all the constituencies have requested studies of various kinds," he said.

Frequent users of Whois were relieved.

Lynn Goodendorf, chief privacy officer for Intercontinental Hotels Group PLC, said that although she was sensitive to privacy concerns that individuals may have, those must be balanced with the needs of businesses and law enforcement officials fighting fraud.

"There are a lot of different wrinkles in this," she said. "The proposal that was on the table to change the policy still had too many potential adverse effects to everyone on the Internet."

Privacy wasn’t a big consideration when the current addressing system started in the 1980s. Back then, government and university researchers who dominated the Internet knew one another and didn’t mind sharing personal details to resolve technical problems.

But the makeup of the Internet population and the use of Whois have changed greatly since then. The requirements for domain name owners to provide such details also contradict, in some cases, European privacy laws that are stricter than those in the United States.

Over the past few years, some companies already have been offering proxy services, for a fee, letting domain name owners list the proxy rather than themselves as the contact. It’s akin to an unlisted phone number, though with questionable legal status.

The rejected proposal, known as operational point of contact, would have made that standard, with fewer restrictions on who could be named as a proxy.

Steve DelBianco, executive director of NetChoice, a coalition of trade groups that represents tech companies, including eBay Inc., Oracle Corp. and Time Warner Inc.’s AOL LLC, said the rise of proxy services shows "the market is working faster to address privacy concerns than ICANN processes ever can."

FTC Says Internet Ad Self-Regulation Falling Short

Internet advertisers have fallen short of promised self-regulation in respecting Internet users’ privacy, a Federal Trade Commission official said on Thursday, even as one firm, Tacoda, said it decided to refrain from collecting some sensitive information.

FTC Commissioner Jon Leibowitz said Internet advertisers should tell consumers that information was being gathered, give them a choice to opt out, and protect any data collected.

"In practice, they often leave a lot to be desired," he said at a FTC conference to discuss the privacy implications of the data collected by Internet advertisers.

The audience was a Who’s Who of Internet advertising firms such as Google Inc and Yahoo as well as privacy advocates.

Leibowitz said his 12-year-old daughter and her friends told him that they been exposed to ads that said things like "touch me harder" and "how long is your next kiss?"

"People should have dominion over their computers," he said. "We really mean it."

He left open the possibility of a "do not track" list, similar to the FTC’s "do not call" registry which requires telemarketers to refrain from phoning anyone on the list. Such a "do not track" list was proposed this week by several consumer and privacy groups.

"I am concerned ... when my personal information is sold to third parties and when my online (research) is tracked across several Web sites," said Leibowitz, one of two Democrats on the five-member commission.

But several other speakers at the FTC conference cautioned against any government regulation.

Randall Rothenberg, president of the Interactive Advertising Bureau, warned against inadvertently stifling one of the most dynamic sectors of the U.S. economy.

"The government must be prudent," he said.

Trevor Hughes of the Network Advertising Initiative mocked what he called the "shock" that advertisers are trying to develop more targeted ads. "We also have self-regulatory programs," he said. "We have many, many layers of control and protection for consumers today."

David Morgan, founder of the advertising firm Tacoda, which was recently acquired by Time Warner’s, said his company considered advertising to children a "third rail" - a reference to the rail that delivers electrical power to a subway train. Touching it means electrocution.

Tacoda shied away from collecting certain sensitive data, even if the Internet user was anonymous, he said.

"The guidance that we’ve gotten is that cancer, HIV, medical conditions, we just stay away from," he said, adding that children’s information and indications of sexual preference also went uncollected.

"We don’t touch search data. You have to filter every bit of it to make sure it’s not personal," he said.

AOL said on Wednesday it would use Tacoda’s technology to let users opt out of online advertisements that are presented to individuals based on the Web sites they have visited.

Google, which has offered $3.1 billion to buy advertising company DoubleClick, is also looking at potential ways to protect consumer privacy.

Behaviorally targeted ads use cookies to track Web sites visited by a consumer so ads can be tailored to that activity.

Bogus FTC E-mail Has Virus

The Federal Trade Commission, which has declared war on Internet scams, warned consumers on Monday not to open a bogus e-mail that appears to come from its fraud department because it carries an attachment that can download a virus.

The e-mail says it is from "frauddep@ftc.gov" and has the FTC’s government seal.

But it was not issued by the agency and has attachments and links that will download a virus that could steal passwords and account numbers, the agency said.

"It’s a treasure trove for identity theft," said David Torok of the FTC’s Bureau of Consumer Protection. "We’re concerned. The virus that’s attached to the e-mail is particularly virulent."

The agency, which is one of several government agencies investigating cyber fraud, did not know how many people had received the e-mail.

"We’ve received hundreds if not thousands of calls and complaints, this one may have had a large distribution," he said.

Recipients should forward the e-mail to spam@uce.gov, an FTC spam database used in investigations.

Nine percent of people surveyed in a poll conducted in August and September reported having had their identities stolen, Bari Abdul, a vice president at security software maker McAfee Inc, said at a cyber security conference on Oct 1.

New Trojan Horse Targets Mac Users

Security research company Intego on Monday issued a security alert about a new Trojan Horse called OSX.RSPlug.A that specifically targets Mac users. The Trojan is a form of DNSChanger that changes the Mac s Domain Name Server (DNS) address.

According to Intego, the Trojan has been found on several pornographic Web sites. When trying to view a movie, the user is told that "Quicktime Player is unable to play movie file. Please click here to download new version of codec."

When the user clicks the link a disk image (.dmg) is downloaded to the desktop. When the user installs the software, they are actually installing the Trojan, not a free video codec. The Trojan is installed with full root privileges, which means it has access to all files and commands on the system.

When the malicious DNS server is active, it hijacks some web requests, leading users to phishing web sites (for sites such as Ebay, PayPal and some banks) or to web pages displaying ads for other pornographic web sites, according to Intego.

The Trojan also installs a root crontab which checks every minute to ensure that its DNS server is still active, the company said. Since changing a network location could change the DNS server, this cron job ensures that, in such a case, the malicious DNS server remains the active server.

Intego says that using Mac OS X 10.4, there is no way to see the changed DNS server in the operating system s interface. Under Mac OS X 10.5, this can be seen in the Advanced Network preferences; the added DNS servers are dimmed, and cannot be removed manually.

Intego has updated its virus definitions to remove the malicious code and prevent it from being installed.

More Spyware-Fighting Tools Needed

Organizations and law enforcement agencies fighting spyware are making progress, but new tools in an antispyware bill stalled in the U.S.

Congress could improve the efforts, a member of the U.S. Federal Trade Commission said Monday.

One of the spyware bills passed by the House of Representatives earlier this year, the Spy Act, would give the FTC authority to impose civil fines on companies that distribute spyware to consumers’ computers. The bill, along with the Internet Spyware Prevention (or I-SPY) Act, have stalled in the Senate since passing the House in May and June.

The FTC has the authority to collect profits from spyware operations and collect money for consumer redress, but it lacks the authority to impose other fines, as it does when going after spammers, said Commissioner Jon Leibowitz, speaking at a spyware forum in Washington, D.C.

Assigning a dollar figure to consumer harm is tricky in many spyware cases, especially when the spyware delivers pop-up advertisements to computers, Leibowitz said. It’s sometimes difficult to get courts to assign large consumer damages to pop-up cases, he said.

In some cases, spyware damages are assessed by judges "who don’t even use computers," said Dave Koehler, with the FTC’s Bureau of Consumer Protection.

The Spy Act would allow the FTC to fine spyware vendors up to $3 million for hijacking computers, delivering unwanted adware, and other violations, and $1 million for collecting personal data without permission, in addition to going after the vendor’s profits and seeking consumer redress.

Additional authority to impose civil fines would give the FTC "an enormous deterrent," Leibowitz said.

"Right now, companies know that the worst they can do is lose their profits," he added. "They’re not going to get fined on top of that."

The FTC has brought several spyware actions against companies. In February, the agency settled a case against adware distributor DirectRevenue. In that case, DirectRevenue settled for $1.5 million, based on its profits, but the founders of the company had received more than $20 million in venture-capital funding, Leibowitz said.

While participants in the spyware forum said there continue to be many challenges, including a growing trend of foreign spyware vendors, the cost of spyware to U.S. consumers seems to be falling. Consumer Reports estimated that spyware cost U.S. consumers $2.6 billion in 2006, but only $1.7 billion in 2007, noted Ari Schwartz, deputy director of the Center for Democracy and Technology, a supporter of StopBadware.org, a consumer-protection effort aimed at spyware and other malicious code.

The drop in the cost of spyware can be attributed to a number of factors, Schwartz said. Antispyware technology is getting better, the FTC has taken action against spyware vendors, and StopBadware.org has distributed a list of malicious Web sites, he said. In addition, some states have taken action against spyware, and cybersecurity groups’ public education programs seem to be working, he said.

But Ron Teixeira, executive director of the National Cyber Security Alliance (NCSA), noted that consumers may know more about spyware, but they aren’t always acting on their knowledge. A survey released by the NCSA and McAfee earlier this month found 78 percent of respondents’ computers didn’t have all three of what the NCSA calls the "core protection" software: anti-virus, antispyware, and firewall.

"We’re not seeing a huge increase in the actual behavior change," he said.

Privacy Groups Seek ’Do Not Track’ List

Nine privacy groups asked the Federal Trade Commission on Oct. 31 to implement a Do Not Track list to prevent consumers from having their online activities unknowingly tracked, stored and used by marketers and advertising networks.

Based on the FTC’s popular Do Not Call list, the Do Not Track list would require advertising firms that place persistent tracking technologies on consumers’ computers to register with the FTC all domain names of the servers involved in such activities. Developers of browser applications would be encouraged to create plug-ins allowing users to download the list onto their computers.

The groups’ call for the Do Not Track list comes on the eve of a two-day FTC conference on "Ehavioral Advertising: Tracking, Targeting and Technology."

"The online tracking and targeting of consumers - both in its current form and as it may develop in the future - needs to be limited so that consumers can exercise meaningful, granular preferences based on timely and contextual disclosures that are understandable on whichever devices consumers choose to use. Consumers must be free to act in their own self-interest," the groups said in a letter to the FTC.

As consumers’ surf the Web, they leave behind information that is currently tracked and targeted, often without their knowledge. Known as "behavioral tracking," the practice collects and compiles a record of individual consumers’ activities, interests and preferences over time.

Federal privacy laws do not cover the practice, although the NAI (National Advertising Initiative), a cooperative of online marketing and analytics companies, promotes a voluntary opt-out system for consumers.

"If you look back at the Do Not Call list, it was at one time managed by industry. But it didn’t gain widespread acceptance until the FTC took it over," Pam Dixon, executive director of the World Privacy Forum, said at an Oct. 31 conference call.

"The industry has had seven years to prove they can manage online opt-outs. It is time to move toward something structured like the Do Not Call list to address the problems we are seeing, and have now seen for seven years."

Dixon called the NAI’s opt-out regime a failure, noting, "We have e-mail that asks us why we have to have a cookie to get rid of cookies. It’s counterintuitive."

The Do Not Track List would still allow companies to place ads, but it would allow consumers to block servers on the list from tracking their online activities. Consumers who sign up for the Do Not Track list would still receive advertising from servers and other technologies that do not employ persistent identifiers.

The privacy groups also want the FTC to adopt an updated definition of "personally identifiable information" and force companies engaged in behavioral tracking to provide consumers with access to the personally identifiable information collected about them. In addition, they are seeking independent audits of behavioral tracking firms to ensure adherence to privacy standards.

"Online opt-outs should be as well-known and as easy as the Do Not Call list," said Mark Cooper, director of research at the Consumer Federation of America.

The nine privacy groups include the Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse and World Privacy Forum.

Group On Non-English Domains Formed

A key Internet oversight agency formed a working group Friday to speed up the process of assigning addresses entirely in other languages.

The decision by the Internet Corporation for Assigned Names and Numbers represents another step toward the approval of internationalized domain names, or IDNs, as early as next year.

The working group will focus on domains for specific countries, such as the Chinese-character equivalent of China’s ".cn" suffix.

"The introduction of the IDNs is absolutely one of the most important changes to the domain name space since its inception," ICANN Chairman Vint Cerf said. "It’s taken many years to get to the point where there is confidence that we understand how to do this."

ICANN started technical tests on such suffixes last month, but work on policy questions is still preliminary.

The organization needs to grapple with how to assign such names and resolve any conflicts or complaints. For example, should the operators of China’s ".cn" automatically be entitled to the Chinese version of that and ".com"? What happens when a competing organization, such as Taiwan’s ".tw" or a private company, wants to claim it?

Those questions could take years to resolve so ICANN is looking at interim procedures that would apply to country-specific domains. The working group was tasked with figuring out how to develop that process. It is to provide a status report in time for ICANN’s February meetings in New Delhi.

Currently ICANN assigns country-specific domains in English based on lists of recognized countries and territories kept by the International Organization for Standardization. ICANN wants to identify a comparable list or other procedures for other languages to avoid having to rule on what is a country and how to pen its name.

Later, ICANN will have to figure out how to permit more generic monikers, such as ".com" in Chinese or Arabic. Those broader policy questions are not part of the working group’s mandate.

Individuals and companies outside the United States long have clamored for non-English scripts, finding restrictive the current limitation of domain names to 37 characters: a-z, 0-9 and the hyphen.

Addresses partly in foreign languages are sometimes possible, but the suffix - the ".com" part of an address - for now requires non-English speakers to type English characters.

As ICANN concluded weeklong meetings in Los Angeles, Cerf said the creation of non-English domains doesn’t necessarily mean more Web sites in other languages.

"It may help content to be discovered but it does not cause it to be created," Cerf said. "So to the extent that we want more content on the network in languages that are native to many populations around the world, we have to encourage people to produce that content. ... This is a completely separate activity, but one without which the Internet and the World Wide Web are far less valuable."

During the meeting, ICANN officials also promised to review the status of domain names applications that were submitted in 2000 but not approved. ICANN never formally rejected them and plans to clarify their status before the next round of applications are solicited, likely next year.

ICANN approved seven out of 47 applications in 2000: ".info" for general information, ".biz" for businesses, ".name" for individuals, ".pro" for professionals, ".museum" for museums, ".coop" for business cooperatives and ".aero" for the aviation industry.

Gossip, E-mailing "All" Among Top Office Peeves

Work colleagues who spend their day gossiping, organizing their home lives, or who press "reply all" on e-mails are among the biggest nuisances in the office, according to a survey released on Monday.

A poll on the biggest pet peeves in the workplace by market researcher Harris Interactive found 60 percent of 2,429 U.S. respondents listed gossip as the biggest annoyance.

The online survey, conducted for staffing firm Randstad USA, found the second biggest peeve at 54 percent was poor time management which included people making personal phones calls at work or surfing the Internet during work time.

Messiness in communal spaces, such as unwashed dishes in the kitchen sinks, irked 45 percent of respondent while potent smells like perfume, food, or smoke, came in fourth in the list with 42 percent.

Rounding out the list of seven office peeves came loud noises such as speaker phones, loud talking and loud phone ring tones at 41 percent, overuse of electronic personal communications devices in meetings at 28 percent and misuse of e-mail at 22 percent.

Eric Buntin, managing director of marketing and operations for Randstad, said the survey indicated people had not changed their behavior as office layouts changed, becoming more open, so people heard colleagues talking and knew more about their home lives.

"If you were sitting in your office with the door closed no one would be able to hear you unless you were very loud but if you open the door then people hear everything, blurring the lines between personal and work lives," Buntin told Reuters.

"People are not taking into account that the workplace is very open now and they need to think about that interaction with their colleagues."

He said the misuse of e-mail was among the top peeves, with people particularly irritated when people e-mailed to "reply all" on an e-mail unnecessarily, or used blind carbon copying (bcc).

"And people who think e-mail is private? No e-mail is private. Everyone knows if they are bcc-ing an e-mail it is like standing up and shouting fire in the middle of a building," he said.

But when it came to taking action against the offending colleagues, people were not so willing to act.

About 42 percent said they would say something directly to a person being too loud but only 34 percent would raise their concerns about gossiping and only 25 percent address a person directly about misuse of e-mail.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.